03-27-00

A/Prov

Dated: March 24, 2000 Our Case Docket No.: MGC 302P

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Assistant Commissioner for Patents
BOX PROVISIONAL PATENT APPLICATION
Washington, D.C. 20231

Sir:

Transmitted herewith for filing is the **PROVISIONAL** patent application of Inventor:
Saqib Jang of Woodside, California

For: SYSTEM AND METHOD FOR SECURITY AND MANAGEMENT OF STREAMING DATA COMMUNICATIONS ON A COMPUTER NETWORK SYSTEM

Enclosed are also:

X 2 sheets of drawings
X Attachment A

PROVISIONAL APPLICATION
SMALL ENTITY

Basic Fee $75.00

Respectfully submitted,

KOLISCH, HARTWELL, DICKINSON,
McCORMACK & HEUSER

J. David Fulmer
Registration No. 42,561
Attorney for Applicant
520 S.W. Yamhill, Suite 200
Portland, Oregon 97204
Telephone: (503) 224-6655
Facsimile: (503) 295-6679

JDF:mmc
Enclosures

"Express Mail" Mailing Label No. EL 543127603US
Date of Deposit - March 24, 2000

I hereby certify that the attached **PROVISIONAL** patent application of Saqib Jang entitled SYSTEM AND METHOD FOR SECURITY AND MANAGEMENT OF STREAMING DATA COMMUNICATIONS ON A COMPUTER NETWORK SYSTEM accompanied by 2 sheets of drawings and an Attachment A is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Mandi Carsey
Mandi M. Carsey

SYSTEM AND METHOD FOR SECURITY AND MANAGEMENT OF STREAMING DATA COMMUNICATIONS ON A COMPUTER NETWORK SYSTEM

Field of the Invention

The present invention relates to the management and security of Internet Protocol (IP)-based streaming data communications, including audio and video communications, within a computer network system.

Brief Description of the Drawings

Fig. 1 is a schematic illustration of an exemplary computer network communications management system in accordance with the present invention implemented in the context of an enterprise network.

Figure 2 is schematic illustration of an exemplary computer network communications management system in accordance with the present invention implemented in the context of Metropolitan Area Network (MAN) Internet Service Provider (ISP) network.

Description of the Invention As Used in an Enterprise Intranet

The invention, indicated generally at 10 in Fig. 1, is a computer software and hardware system that provides enhanced management and security capabilities to network administrators. Those of skill in the art will appreciate that the invention may be implemented in the context of a variety of network architectures, including as a component of an enterprise or Internet Service Provider (ISP) network. In the exemplary implementation of the invention implemented in the context of an enterprise network depicted in Fig. 1, the invention is configured "co-edged" or parallel to the enterprise network firewall to enable high-performance and secure deployment of streaming media across the enterprise network in a firewall-independent fashion. The invention acts as a specialized high-performance security and management system for Internet Protocol (IP) streaming media, allowing a administrator to impose fine-grain and more application-specific control over the way in which such data is deployed within an enterprise extranet, while providing the required data throughput for broad-based deployment of such bandwidth-intensive data within the enterprise.

In the exemplary implementation depicted in Fig. 1, system 10 works by acting as a high-performance streaming data switch in establishing network communications between internal (i.e. within the enterprise network) and external streaming application end-points, such as IP videoconferencing group or desktop stations. The streaming data firewall function of system 10 implements a dynamic port management capability, opening and closing ports only as needed during streaming calls, and selectively transporting this data across the proxy, based upon security policies previously defined by the security administrator. The result is that deployment of streaming data within the enterprise is accomplished in a high-performance, secure, and firewall-independent way.

The network firewall is not required to open any additional ports for streaming media therefore making the firewall less vulnerable versus the alternative solution of having streaming data traverse the firewall. Further, any impact on the performance of streaming applications due to firewall performance limitations in handling streaming traffic is minimized. Finally, any impact on the performance of the network firewall is minimized versus the alternative approach of having streaming data traverse the firewall.

As will be appreciated by those of skill in the art, a firewall engenders confidence in network security by centralizing the management and control of an enterprise's security policies for commonly used data protocols, such as Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP). While firewalls may also provide some level of security for streaming protocols, such as those based on the Real Time Streaming Protocol (RTSP), the complexity and performance-intensive nature of such protocols is such that administrators typically disable or limit firewalls from transporting streaming data. However, the design of System 10 enables high-performance, secure, and enterprise-wide deployment of streaming media by off-loading transporting of streaming data from firewalls and by providing a specialized, high-performance proxy service that provides administrators with the ability to impose more powerful security policies having a higher resolution for streaming traffic than that provided by typical firewalls.

System 10 typically provides a range of general functions for supporting security and management for streaming data. These component functions are illustrated schematically in Fig. 1. It will be appreciated that Fig. 1 is a functional overview of an exemplary embodiment and deployment scenarios of system 10, and does not necessarily reflect its use in other scenarios (such as a component of an Internet Service Provider network as depicted in Fig. 2 which is described later).

First, the system provides a specialized firewall service for secure incoming (i.e. initiated by external streaming end-points) and outgoing (i.e. initiated by internal end-points) call set-up and data exchange of streaming traffic. Note that the term "end-point" can refer to individual user desktop systems, group conference room audio/video stations and multipoint systems (Multipoint Control Units (MCU) in H.323 parlance) which mix audio streams and provide video selection for individual end-points for multiparty calls. The firewall component includes a streaming proxy capability designed to provide security for streaming data calls (for example that using RTSP-based protocols, such as H.323 and Session Initiation Protocol (SIP)) among internal and external users. External end-points initiate calls to internal end-points by directly connecting to the streaming proxy component of the firewall service by using the proxy's fully qualified Domain Name Service (DNS) name, globally unique IP address or by accessing proxy addressing information via an external Address Resolution Service, such as Microsoft User Locator Service or an X.500 Directory Service. The enterprise edge router system is configured to transport any traffic destined for, or originating from, the IP address of system 10 such as the connect request from the external end-point. External end-points include information, such as its E.164 address (i.e. a phone number), arbitrary alias name string or Domain Name Service (DNS) name, about the target internal user or end-point in the proxy connect request. The proxy resolves this information into a valid IP address. In the case of H.323 calls, the proxy uses the gatekeeper (which maintains a database of H.323 endpoints in the enterprise network and their aliases) within system 10 for the E.164 or alias name to IP address translation. Next, the proxy uses the resolved IP address of the target desktop to setup a connection between the external and internal endpoints for exchange of audio/video data. The proxy component also includes the capability to dynamically open and close Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) corresponding to individual call set-up and streaming data exchange communication flows for the duration of each call.

The second component of system 10 is an optimized Network Address Translation (NAT) service for streaming data. NAT functionality is common in standard firewalls as a means of mapping globally unique IP addresses used on the Internet to private IP addresses used on the Intranet. NAT systems work by parsing the header IP packets of traffic flowing between the intranet and external Internet and making the appropriate substitutions. However, this approach does not work in the case of streaming data traffic, such as H.323 and SIP applications, as such streaming applications pass IP address and port number information both in the IP packet header and payload. The specialized NAT service within system 10 will make the necessary global address to private address (and vice-versa) substitutions both in the packet header and payload.

The third component of system 10 is a streaming policy engine that provides fine-grained policies for managing the security and network bandwidth utilization for streaming traffic. It accomplishes this by providing flexible, easy-to-use and secure local and remote Graphical User Interfaces (GUIs) for dynamic policy management using a variety of IP-level and application protocol (e.g. H.323 and SIP)-specific parameters for individual streaming data calls. Specifically, the policy engine enables administrators to control for individual calls:

- who (identified by user-level authentication and/or machine IP address parameters) among internal users can initiate streaming data calls)
- who can receive video calls from external users and end-points
- who can participate in streaming data calls versus who can only listen
- the maximum bandwidth each individual user can use to initiate or receive streaming data calls
- who is limited to accessing audio data for audio/video calls
- who can receive and/or initiate calls during specific times of day
- Which users' calls require encryption
- What external users and/or endpoints (identified by IP address and user authentication information) can internal users connect to or will calls be accepted from?

The four component system of system 10 is Quality of Service (QoS) services for streaming data. QoS services incorporate standard mechanisms that allow network equipment deployed within enterprise and Internet Service Provider networks to provide preferential treatment to real-time traffic, such as streaming audio and video traffic, as well as Service Level Agreement (SLA) agreement monitoring of streaming data flows supported by the switch. These standard mechanisms include:

- Multi-protocol Label Switching (MPLS), an Internet Engineering Task Force (IETF) standard, that presents a simple way to forward information through networks by installing and then examining short, fixed-length ID markings called labels in packets. By relying on labels to forward information, MPLS usually doesn't use a packet's IP header unless it is entering or leaving MPLS-enabled. The QoS service allows system 10 to install and remove labels in streaming packet flows as such data is forwarded or received from ISP networks respectively.
- Diff-Serv (Differentiated Services) is also an IETF standard for "tagging" packets for special treatment as they traverse the public Internet. Specifically, it encodes the Type-of-Service (TOS) bits in the header of an IP packet to denote the level of service the packet should receive. The QoS service allows system 10 to optionally encode the TOS bits to allow the network equipment within ISP networks to provide preferential treatment to streaming data traffic.

SLA monitoring and reporting is the additional capability of the system's QoS services. This capability allows administrators to get periodic or ad-hoc reports of the following types of information for individual streaming data calls: bandwidth utilization, mean/median packet latency, jitter (latency variation), and packet loss. These reports enable administrators of enterprise and ISP networks to ensure compliance of streaming data traffic with Service Level Agreements agreed upon between ISPs and enterprises.

System 10 also incorporates a streaming data encryption module. The function of the encryption module is to optionally encrypt video communication flows. Encryption modules in two instances of system 10 each deployed either in an enterprise or ISP network work in conjunction to encrypt or decrypt streaming traffic.

System 10 also includes a bandwidth management module. The function of this module is to allow administrators to easily provision the maximum bandwidth of streaming data traffic for an enterprise network. The bandwidth management module also allows setting of bandwidth parameters on a per-user basis, by time of day and by source and destination IP address for a streaming data call. The result is that this module, in conjunction with the streaming data policy engine module, allows fine-grain management of the impact of streaming data bandwidth on overall enterprise network bandwidth.

The seventh component of system 10 is a wire-speed switching fabric enabling transporting of streaming data traffic across system with zero appreciable latency, even as the streaming data traffic is parsed and analyzed by system 10 to impose policies and provide optional encryption. Measurements indicate that one implementation of system 10 can provide aggregate streaming data throughout of up to 1.048 Gbps with full policy management, QoS, and encryption support. The wire-speed switching fabric includes full support for IETF standard IP routing protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Routing Information Protocol (RIP). Support of these routing protocols will allow system 10 optionally to support a dedicated high-speed Internet connection for streaming data traffic.

System 10 also includes two applications: a Services Management System (SMS) that allows Internet Service Providers (ISPs) to easily deliver, provision, account for and maintain IP-based streaming data services. In the scenario depicted in Fig. 1 the SMS application running remotely on a UNIX, NT or Windows workstation provides SPs with comprehensive network management functionality, including fault, configuration, accounting, performance and security monitoring for one of system 10 instances. The second application is a Subscriber Network Management (SNM) application for the enterprise subscriber. This is a browser-based customer-care system for the subscriber site that provides enterprise network managers with visibility and control into their portion of the Internet Service Provider's (ISP's) network. Subscribers get a unique view of their service, regular updates on network performance compare to Service Level Agreement (SLA) commitments and the tools to adjust services to meet the rapidly changing needs of the business.

System 10 also provides an open API allowing it to serve as a platform for end-customer or 3rd party developed value-added streaming data applications. The API provides the ability, for example, to develop store-and-forward applications, such as video mail, and value-added interactive video applications such as:

- Transcoding H.323 traffic into RealMediaG2 protocol format enabling desktop users to participate in videoconferences

- Two instances of system 10 can work together to provide unicast to multicast (and vice-versa) translation enabling bandwidth-efficient streaming data communication within the enterprise network while deliver unicast data for delivery over the global Internet.

Description of the Invention As Used in an Internet Service Provider Network

While Fig. 2 illustrates the deployment of system 10 as part of an Metropolitan Area Network (MAN) Digital Subscriber Loop (DSL) Internet Service Provider network, those of skill in the art will appreciate that the invention may be implemented in the context of a variety of ISP network architectures, including being deployed in a Competitive Local Exchange Carrier (CLEC) Central Office (CO) or a Tier 1 long-haul (US-wide or global) ISP network.

The range of functions supported by system 10 (as described in the earlier section) continue to be applicable in the context of Figure 2 with one important distinction. In contrast to the earlier case, system 10 enables MAN providers to deliver streaming data services in a high-performance, secure, and manageable fashion to *multiple* enterprise subscribers.

These carriers can use DSL to provide secure IP-based streaming data services, such as IP videoconferencing, in the same way that these services can be provided via private line, Frame Relay and dial access services. The DSL concentrators located at the carrier network access points efficiently process traffic from each DSL subscriber site and transmit it over Frame Relay or ATM to an instance of system 10, where a variety of value-added IP streaming data services, such as IP videoconferencing services, can be applied to each subscriber's network connection. Carriers utilizing system 10 can leverage existing infrastructure to offer various streaming data features that address a broad base of customer requirements, including the following:

- Site-to-site IP videoconferencing services: the ability to create high-performance, secure interactive audio/video links between offices
- Remote access IP video services: the ability to create IP audio/video connections for mobile workers
- Extranet IP video services: the ability to create secure IP interactive audio/video links for suppliers, partners, and customers

A value-added capability that carriers can offer using system 10 is managed firewalls for streaming data. Many small and medium-sized businesses implementing DSL are migrating from analog or digital dial-up connections and are concerned with the heightened security risks associated with an "always-on" connection. The security concerns are even stronger as these business envision migrating from point-to-point digital dial-up connections, such as Integrated Digital Services Network (ISDN), to DSL-based IP connections for streaming data applications such as IP videoconferencing applications. System 10 provides network-based firewalls, a more scalable and manageable alternative to implementing customer premises equipment (CPE)-based firewalls. System 10 supports encryption services for streaming data for additional, optional security.

Carriers can provision any of the new system 10-enabled IP streaming data services without changing existing equipment or software at the customer site. The system's unique ability to support hundreds to thousands of virtual subscriber interfaces and IPSec encryption services allows carriers to offer differentiated DSL streaming services in new markets with less investment in new equipment. Value-added services can be applied to DSL customer traffic and securely transported over the Internet.

As shown in the embodiment of system 10 in a DSL MAN network, system 10 is deployed at the point providing access to the MAN network to multiple subscribers, typically a network Point of Presence (POP) or Central Office (CO). The MAN DSL carrier will use system 10 to offer specialized streaming data services, such as IP videoconferencing services to the customers over a DSL line into the customer premises. In the case of the streaming data service being provided over a DSL line to an individual subscriber, the firewall services component of system 10 will ensure the security of this connection and will only allow valid (authorized) streaming data to traverse this DSL connection for inbound or outbound access into the subscriber network. Each of the other components of the system can be used by ISPs to deliver, provision, and account for streaming data services for individual subscribers in a high-performance, secure, and policy-based way. As illustrated in Fig. 2, each system 10 deployed in a POP location provides high-performance, security, and policy management for streaming data traffic for multiple subscribers. Each of the components of system 10 (as discussed in the earlier section) include capabilities to segment streaming data traffic for multiple subscribers enabling system 10 to concurrently deliver streaming data services to hundreds to thousands of subscribers.